

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

TEVA PHARMACEUTICALS USA, INC. : CIVIL ACTION

v. :

**BARINDER SANDHU, JEREMY DESAI,
APOTEX INC. and APOTEX CORP. : NO. 17-3031**

MEMORANDUM OPINION

Savage, J.

January 30, 2018

This misappropriation of trade secrets action requires us to decide two issues arising under the Computer Fraud and Abuse Act (CFAA) that have split the circuit courts and the Third Circuit has yet to address. First, can an employee who misuses information she was authorized to access be held liable? Second, may a plaintiff only recover losses caused by an interruption of service? Stated differently, can the plaintiff recover losses that are not linked to an interruption of service? We answer the first question in the negative, and the second in the affirmative.

Teva alleges that its former employee, Barinder Sandhu, passed trade secrets to her romantic partner, Jeremy Desai, the CEO of Apotex, its competitor. Tipped off that Sandhu had transmitted confidential documents to Apotex, Teva conducted an internal investigation that confirmed the tip. Teva then terminated her and filed this action against Sandhu, Apotex, and Desai for computer fraud under federal law, misappropriation of trade secrets under federal and state law, and state law tort claims.

Sandhu, Apotex, and Desai move to dismiss the complaint, arguing that Teva fails to allege facts giving rise to a claim for relief. Teva sufficiently pleads that its trade secrets were misappropriated; Sandhu converted its trade secrets and breached her

employment contract and her fiduciary duty; and Desai and Apotex procured information by improper means, tortuously interfered with Sandhu's employment contract, and aided and abetted her breach of fiduciary duty owed to Teva. Because it fails to plead that Sandhu's accessing its computer system was without authorization or exceeded her authorization, Teva's claim under the CFAA against Sandhu is dismissed. Therefore, we shall grant the motions in part and deny them in part.

Factual Background

From June 25, 2012 until October 11, 2016, Sandhu worked at Teva in Regulatory Affairs.¹ From May 2014 until her termination, she was Senior Director, overseeing the post-approval regulatory affairs for U.S. generic products.² When she joined Teva, she signed a confidentiality agreement prohibiting her from improperly disclosing trade secrets or confidential information.³ During her employment at Teva, Sandhu was in a romantic relationship with Desai, the CEO of Apotex, a competing pharmaceutical company.⁴

Sometime in the summer of 2016, Teva learned from a former Apotex employee that Sandhu had shared confidential information about its products in development with Desai.⁵ One of the documents was a Complete Response Letter (CRL) for one of Teva's generic drug products. The CRL includes confidential correspondence from the

¹ Compl. (Doc. No. 1) ¶¶ 33, 38, 81. The facts recited are those alleged in the complaint.

² *Id.* ¶ 44.

³ *Id.* ¶¶ 48–53.

⁴ *Id.* ¶ 5.

⁵ *Id.* ¶ 56.

Food & Drug Administration (FDA) regarding how a new drug may gain approval.⁶ Teva claims that Apotex used information in the CRL to advance the market position of its competing generic product and that it continues to use the information to inform its purchasing decisions, set production goals, and increase its visibility in the market.⁷

Acting on the tip, Teva conducted an internal investigation, searching Sandhu's company-issued laptop and email account.⁸ The investigation revealed that Sandhu had emailed documents marked as "confidential" and containing trade secrets to Desai at his Apotex email address.⁹ On her work laptop was a folder containing approximately 900 Teva files copied to her personal cloud-based repository, allowing her to access the files from anywhere.¹⁰ A document uploaded to the folder on August 8, 2016 contained information on the regulatory status of pre-approval and post-approval products, and notes on communications with the FDA regarding Teva's active drug submissions.¹¹ The investigation also revealed that Sandhu had downloaded documents from the folder to USB drives.¹² As a result, she was terminated on October 11, 2016.¹³

Teva then brought this action. It brings a claim under the CFAA for unauthorized access of its protected computers. It contends that Sandhu, Desai, and Apotex

⁶ *Id.* ¶¶ 56–58.

⁷ *Id.* ¶¶ 59–61; Teva Resp. to Apotex Mot. to Dismiss (Doc. No. 47) at 7, ECF 15.

⁸ Compl. ¶¶ 64, 81.

⁹ *Id.* ¶ 66.

¹⁰ *Id.* ¶¶ 67–68.

¹¹ *Id.* ¶ 70.

¹² *Id.* ¶¶ 75–80.

¹³ *Id.* ¶ 81.

misappropriated its trade secrets in violation of the Defend Trade Secrets Act (DTSA) and the Pennsylvania Uniform Trade Secrets Act (PUTSA). Teva also asserts state law tort claims for conversion and procuring information by improper means against all defendants; breaches of contract and fiduciary duty against Sandhu; aiding and abetting a breach of fiduciary duty against Apotex and Desai, tortious interference with contractual relations against Apotex and Desai; and unfair competition against Apotex. In addition to demanding compensatory and punitive damages, Teva seeks to enjoin all defendants from retaining and using its improperly acquired trade secrets and confidential information.

Standard of Review

A Rule 12(b)(6) motion tests the sufficiency of the allegations contained in the complaint. In order to survive a Rule 12(b)(6) motion, “a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is plausible “when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Iqbal*, 556 U.S. at 678.

A conclusory recitation of the elements of a cause of action is not sufficient. *Phillips v. Cty. of Allegheny*, 515 F.3d 224, 233 (3d Cir. 2008). The plaintiff must allege facts necessary to make out each element. *Id.* (quoting *Twombly*, 550 U.S. at 563 n.8). In other words, the complaint must contain facts which, if proven later, support a conclusion that a cause of action can be established.

All well-pleaded allegations of the complaint must be accepted as true and

interpreted in the light most favorable to the plaintiff, and all inferences must be drawn in the plaintiff's favor. See *McTernan v. City of York*, 577 F.3d 521, 526 (3d Cir. 2009).

Computer Fraud and Abuse Act (CFAA)

The CFAA imposes civil liability on anyone who knowingly "accesses a protected computer without authorization, or exceeds authorized access" of a protected computer. 18 U.S.C. § 1030(a)(4). To state a CFAA claim, a plaintiff must show that the defendant: (1) accessed a "protected computer;" (2) without authorization or exceeded authorized access; (3) knowingly and with an intent to defraud; (4) obtained something of value; and (5) caused damage or loss to the plaintiff in excess of \$5,000 in a one-year period. *Synthes, Inc. v. Emerge Med., Inc.*, Civ. A. No. 11-1566, 2012 WL 4205476, at *15 (E.D. Pa. Sept. 19, 2012) (quoting 18 U.S.C. § 1030(a)(4)); see also *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 510 (3d Cir. 2005).

The defendants argue that Teva has not stated a claim under the CFAA because it has failed to plead that Desai and Apotex accessed Teva's computers, that Sandhu exceeded her authorized access to Teva's computers, and that Teva suffered a recoverable loss. Desai and Apotex also contend that Teva fails to plead that its computers are statutorily protected.

Because Teva does not allege that Sandhu acted without authorization or exceeded her authorized access, the CFAA claim against her must be dismissed. On the other hand, the CFAA claims against Desai and Apotex survive under a theory of indirect unauthorized access.

Protected Computer

A protected computer is one that “is used in or affecting interstate or foreign commerce or communication.” 18 U.S.C. § 1030(e)(2)(B). A computer is “protected” if it is connected to the Internet. *United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007) (quoting *United States v. MacEwan*, 445 F.3d 237, 245 (3d Cir. 2006)).

The complaint clearly alleges that the computer Sandhu accessed was connected to the Internet and used in interstate communication. Teva’s global headquarters is in Pennsylvania, where Sandhu resided and from where she transmitted the trade secrets to Desai in Canada. Apotex, the ultimate recipient of the information, is a Canadian corporation based in Toronto.¹⁴ Thus, contrary to Apotex and Desai’s contention,¹⁵ Teva sufficiently alleges facts demonstrating that its computers are protected under the CFAA.

Access

The CFAA does not define “access.” Nor does it define “without authorization.” The statute defines “exceeds authorized access” as “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.” 18 U.S.C. § 1030(e)(6). In other words, the statute imposes liability on one who acts beyond the scope of her access authority.

¹⁴ *Id.* ¶¶ 25–28. Apotex’s U.S. subsidiary is a Delaware corporation headquartered in Florida. *Id.* ¶ 29.

¹⁵ Apotex Mot. to Dismiss at 18, ECF 23. Desai “joins and incorporates” all of Apotex’s arguments in its motion as they apply to him. See generally Desai Mot. to Dismiss (Doc. No. 49-1).

How to apply the definition of “exceeds authorized access” under section 1030(a)(4) of the CFAA when it is an employee who properly accessed and improperly used the information has split the circuit courts. The division has resulted in two views of the reach of the employee’s authorization. Under the narrow approach, employees who misuse information they obtained through authorized access are not subject to liability. The broad approach holds them liable.

The Fourth and the Ninth Circuits construe the statute narrowly. See *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012); *United States v. Nosal*, 676 F.3d 854, 857 (9th Cir. 2012) (en banc); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009). Literally interpreting the statute, they conclude that the statute prohibits unauthorized access and does not extend to the use of the information accessed. In other words, liability attaches to access, not use. Thus, according to this narrow view, an employee cannot be liable for misusing the information she was authorized to obtain.

The First, Fifth, Seventh, and Eleventh Circuits interpret the statute broadly, treating employees the same as any other persons who misuse information obtained from a computer. They hold them liable even though they were authorized to obtain the information. See *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010); *United States v. John*, 597 F.3d 263, 271–72 (5th Cir. 2010); *Int’l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420–21 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581–83 (1st Cir. 2001). These courts focus on use, not access. They reason that the employee’s access authority terminates upon her breach of the fiduciary duty owed to her employer. In these cases, the duty was created by the employer’s

express policy or the employee's written agreement not to disclose or misuse the information provided by access to the employer's computers. See *Citrin*, 440 F.3d at 420–21.

The Third Circuit has yet to address the issue. Courts within this district universally subscribe to the narrow approach, barring liability where the employee has authorization to access the computer to obtain the information.¹⁶

In interpreting a statute, we start with the plain language. *Kingdomware Techs., Inc. v. United States*, 136 S. Ct. 1969, 1976 (2016). If the language is clear and unambiguous, the inquiry is complete. *Id.*; see also *Matal v. Tam*, 137 S. Ct. 1744, 1756 (2017) (citation omitted). In that case, there is no need to resort to legislative history or any other extrinsic material. *Parker v. NutriSystem, Inc.*, 620 F.3d 274, 277 (3d Cir. 2010). On the other hand, where the language is ambiguous, we ascertain the intent of Congress by examining the statutory purpose and legislative history. *Id.* at 278.

In determining whether language is ambiguous, we “read the statute in its ordinary and natural sense.” *In re Harvard Indus., Inc. v. IRS*, 568 F.3d 444, 451 (3d Cir. 2009) (citation omitted). A provision is ambiguous when there is reasonable disagreement as to its meaning. *N.L.R.B. v. New Vista Nursing & Rehab.*, 719 F.3d

¹⁶ See, e.g., *Brand Energy & Infrastructure Servs., Inc. v. Irex Contracting Grp.*, Civ. A. No. 16-2499, 2017 WL 1105648, at *14 (E.D. Pa. Mar. 24, 2017) (Stengel, J.) (citing *Kappe Assocs., Inc. v. Chesapeake Environ. Equip., LLC*, Civ. A. No. No. 15-2211, 2016 WL 1257665, at *8 (E.D. Pa. Mar. 31, 2016) (Leeson, J.); *Dresser-Rand Co. v. Jones*, 957 F. Supp. 2d 610, 616–19 (E.D. Pa. 2013); *Grant Mfg. & Alloying, Inc. v. McIlvain*, Civ. A. No. 10-1029, 2011 WL 4467767, at *6–7 (E.D. Pa. Sept. 23, 2011) (Sánchez, J.), aff'd, 499 Fed. App'x 157 (3d Cir. 2012); *Clinton Plumbing & Heating of Trenton, Inc. v. Ciacco*, Civ. A. No. 09-2751, 2010 WL 4224473, at *5 (E.D. Pa. Oct. 22, 2010) (Rufe, J.); *Integrated Waste Solutions, Inc. v. Goverdhanam*, Civ. A. No. 10-2155, 2010 WL 4910176, at *8 (E.D. Pa. Nov. 30, 2010) (Buckwalter, J.); *Bro-Tech Corp. v. Thermax, Inc.*, 651 F. Supp. 2d 378, 407 (E.D. Pa. 2009) (Rufe, J.); *Brett Senior & Assocs., P.C. v. Fitzgerald*, Civ. A. No. 06-1412, 2007 WL 2043377, at *3 (E.D. Pa. July 13, 2007) (McLaughlin, J.)).

203, 226 (3d Cir. 2013) (quoting *Dobrek v. Phelan*, 419 F.3d 259, 264 (3d Cir. 2005)). However, because courts interpret a statute differently does not create an ambiguity. *In re Friedman's Inc.*, 738 F.3d 547, 554 (3d Cir. 2013).

The statute defines “exceeds authorized access” as “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.” 18 U.S.C. § 1030(e)(6). It does not define “authorization.”

Because the statute does not define “authorization,” “we construe it in accordance with its ordinary meaning.” *United States v. Husmann*, 765 F.3d 169, 173 (3d Cir. 2014) (quoting *Octane Fitness, LLC v. ICON Health & Fitness, Inc.*, 134 S. Ct. 1749, 1756 (2014)). Looking to the dictionary definition to determine its ordinary meaning, authorization means “formal permission or approval” or “sanction.” Oxford English Dictionary (2d ed. 2012); Webster’s 3d New Int’l Dictionary, Unabridged (2018); see also Black’s Law Dictionary (10th ed. 2014).

Applying this definition to the statutory framework, an employee is “authorized to access a computer when his employer approves or sanctions his admission to that computer.” *Dresser-Rand*, 957 F. Supp. 2d at 617 (quoting *WEC Carolina*, 687 F.3d at 204). An employee is “without authorization” when “he gains admission to a computer without approval,” *id.*, that is, where initial access is not permitted. See also *Diamond Power Int’l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1342 (N.D. Ga. 2007). An employee may have authority to access the computer, but not to obtain certain information once access has been gained. In that instance, the employee is liable for

exceeding authority. The definition does not cover the use of the information once properly obtained.

The statute, read plainly, does not ensnare a person who was authorized to obtain information in the computer, but was not authorized to use it the way she did. Had Congress intended the statute to punish one who misuses information she was authorized to obtain, it knew how to do so. It could have added one word—"use"—to the statute, so it would read, "to access a computer with authorization and to use such access to obtain[, use,] or alter information in the computer that the accesser is not entitled so to obtain[, use,] or alter."

Courts subscribing to the broad approach expand the scope of the statute beyond what Congress intended. See, e.g., S. Rep. 99-432, at 3 (1986); see also *Nosal*, 676 F.3d at 863 (citations omitted). They base their reasoning on a breach of fiduciary duty, which is not an element of a CFAA violation. Instead, it is an element of a separate cause of action—a state law breach of fiduciary duty.

"Exceeds authorized access" means obtaining information beyond what was authorized. It does not go to the improper use of the information validly accessed. *WEC Carolina*, 687 F.3d at 204. It goes to obtaining information that was not within the scope of the authorization. Thus, an employee who misuses information she was authorized to obtain cannot be held liable. *Id.*

In *WEC Carolina*, a WEC employee emailed confidential documents he had downloaded to his personal account before resigning from the company to work for a competitor. *Id.* at 202. After leaving WEC, the former employee used the information in a presentation aimed at attracting a potential WEC customer. *Id.* The potential

customer hired the competitor instead of WEC. *Id.* Similar to the facts Teva alleges here, WEC had a policy prohibiting unauthorized use of confidential information or trade secrets, including the downloading of confidential information to a personal computer. *Id.* at 206–07. In its complaint, WEC conceded that its former employee was authorized to access its computer system at the time he downloaded and emailed the confidential information. *Id.* at 207. The Fourth Circuit affirmed the district court’s dismissal of the CFAA claim because the employer failed to allege that its former employee had exceeded his authorized access. *Id.*

The Fourth Circuit held that an employee exceeds his authorized access “when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access.” *Id.* at 204 (citing *Brekka*, 581 F.3d at 1133). The court noted that this definition does not extend “to the improper use of information validly accessed.” *Id.* (emphasis in original).

Under this narrow approach we adopt, Teva fails to state a claim against Sandhu. She was permitted to access the Teva computer in the course of her employment to obtain information in its database, including the information she allegedly shared with Desai and Apotex. Because she was authorized to access Teva’s computers when she did, any subsequent misuse of the information is not actionable. See, e.g., *id.*; *Brekka*, 581 F.3d at 1135; *Brand Energy*, 2017 WL 1105648, at *14 (citation omitted). Hence, because Sandhu did not obtain the information at issue without authorization or beyond her authorized access, we shall dismiss the CFAA claim against her.

Outsiders, like Apotex and Desai, are not treated the same as insiders. Rather, they are akin to hackers, those the CFAA aimed to hold criminally and civilly liable. They did not have authority to access the computers. But, they indirectly accessed Teva's protected computers through one who had the authority. They knew the information they obtained had been purloined through accessing Teva's computers.

A person who did not directly access the computer may still be liable under the CFAA if he "directs, encourages, or induces" someone else to access a computer that he himself is unauthorized to access. *Brand Energy*, 2017 WL 1105648, at *14 (citing *Huber*, 28 F. Supp. 3d at 327). The CFAA does not specify that liability attaches only to one who directly accesses the computer. One who is not authorized to access the information may gain access through one who has access authority, giving rise to liability for indirect access. *Id.* (quoting *Synthes*, 2012 WL 4205476, at *17) ("no modifying term suggesting the need for 'personal access' is included" in the definition of access).

Teva alleges that Desai and Apotex, who were not authorized to do so, acted in concert with Sandhu, an employee at Teva, to access its protected computers.¹⁷ It contends that Desai and Apotex, "knowing that the information shared with them by Sandhu was Teva[s] trade secrets," then used the information "to increase their competitive advantage" and profits.¹⁸ These allegations state a CFAA claim against Apotex and Desai based upon an indirect-access theory.

¹⁷ Compl. ¶ 27.

¹⁸ *Id.* ¶¶ 104–05.

Loss

Loss under the CFAA “means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11). The parties disagree whether only loss caused by an interruption of service is recoverable.

The only circuit courts to address the issue have held that not every loss need be tethered to an interruption of service. No circuit court has held otherwise. The Fourth, Sixth, and Eleventh Circuits conclude that the plain language of the statutory definition includes two separate categories of loss because the loss provision is “written in the disjunctive.” *Brown Jordan Int’l, Inc. v. Carmicle*, 846 F.3d 1167, 1174 (11th Cir. 2017) (citation omitted); *Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*, 774 F.3d 1065, 1073–74 (6th Cir. 2014); *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009). As interpreted by these courts, there are two categories of loss. The first type of loss—direct costs of responding to a violation—is recoverable “irrespective of whether there was an interruption of service.” *Brown Jordan Int’l*, 846 F.3d at 1174 (citing *Yoder*, 774 F.3d at 1073–74; *iParadigms*, 562 F.3d at 646). The second type of loss—consequential damages—is recoverable only if resulting from an interruption of service. *Id.* Several district courts, on the other hand, have concluded that recoverable loss must be related to an interruption of service of a computer or computer system.¹⁹

¹⁹ See, e.g., *Advanced Fluid Sys., Inc. v. Huber*, 28 F. Supp. 3d 306, 330 (M.D. Pa. 2014) (quoting *Brooks v. AM Resorts, LLC*, 954 F. Supp. 2d 331, 337–38 (E.D. Pa. 2013) (collecting cases)).

We agree with the circuit courts that interpret loss as composed of two distinct categories. Section 1030(e)(11) is comprised of two dependent clauses, separated by the word “and.”²⁰ There are two separate, independent series in the definition—direct costs related to addressing a violation, and consequential damages resulting from an interruption of service.

The different interpretations arise from the effect of the last five words of the definition, the phrase “because of interruption of service.” What the phrase modifies is the source of the different interpretations. It is a postpositive modifier because it is positioned after what it modifies. A. Scalia & B. Garner, *Reading Law: The Interpretation of Legal Texts* at 148 (2012).

A postpositive modifier may not apply to multiple series when the statutory language also includes a determiner—a modifying word that introduces and provides context to the word or words it modifies. When a determiner, such as “any,”²¹ is repeated at the beginning of the second series, the syntax suggests that the postpositive modifier does not operate to modify both series. *Id.* at 150 (citing *United*

These courts reason that requiring an interruption of service is consistent with the legislative intent of the CFAA—a criminal statute intended to address interruption of service and damage to protected computers. See, e.g., *Von Holdt v. A-1 Tool Corp.*, 714 F. Supp. 2d 863, 876 (N.D. Ill. 2010) (quoting *Cont'l Grp., Inc. v. KW Prop. Mgmt., LLC*, 622 F. Supp. 2d 1357, 1371 (S.D. Fla. 2009)).

They explain that interpreting loss as composed of two distinct categories reduces the second half of the definition to surplusage. See, e.g., *Cont'l Grp.*, 662 F. Supp. 2d at 1371 (“If loss could be any reasonable cost without any interruption of service, then why would there even be a second half to the definition that limits some costs to an interruption of service.”). As the Eleventh Circuit explained in *Brown Jordan Int'l*, the “interruption of service” language is not mere surplusage. 846 F.3d at 1174. To the contrary, it is the cause of the second category of recoverable loss. *Id.*

²⁰ Loss “means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, **and** any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11) (emphasis added).

²¹ “Any” is a determiner that quantifies the noun it modifies.

States v. Pritchett, 470 F.3d 455, 459 (D.C. Cir. 1972)). Instead, it modifies only the series immediately after which it is positioned.

Here, the definition of loss is comprised of two series, each beginning with the determiner “any.” In other words, appearing a second time in the definition, “any” signals the beginning of a second series. The two series are separated by “and,” and each is introduced by “any.” The first series consists of “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense.” In the first series, there are three examples of “any reasonable cost,” which are introduced by “including,” connoting a non-exhaustive list. The second series is “any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.”

The postpositive modifier “because of interruption of service” appears at the end of the second series. The syntax suggests that it modifies only the second series because the determiner “any” signals the start of the second series, which begins after the word “and.” See Scalia & Garner, *Reading Law* at 148–50 (citing *Pritchett*, 470 F.2d at 459). Thus, only the loss described in the second series must be caused by an interruption of service, and loss described in the first series is recoverable with or without service interruption.

Although we conclude the statutory language creates two categories of loss, there is reasonable disagreement as to its meaning. Accordingly, we examine the legislative history to discern congressional intent.

What Congress intended has also engendered disagreement. Courts examining the legislative history have reached opposite conclusions on Congress's intent in defining loss. *Compare, e.g., Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*, Civ. A. No. 3:10 CV 1590, 2011 WL 2433504, at *4 (N.D. Ohio June 14, 2011), *aff'd*, 774 F.3d 1065 (6th Cir. 2014); *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 475 (S.D.N.Y. 2004), *aff'd*, 166 F. App'x 559 (2d Cir. 2006); *NCMIC Fin. Corp. v. Artino*, 638 F. Supp. 2d 1042, 1064 (S.D. Iowa 2009), *with, e.g., Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1126–27 (W.D. Wash. 2000).

Unfortunately, the legislative history provides no guidance to discern Congress's intent in defining loss. Loss was not defined in the CFAA until the statute was amended in 2001. There is a dearth of legislative history associated with the 2001 amendment. In the only relevant statement describing the amendment, Congress discussed the scope of losses recoverable as those incurred "responding to a computer hacker." 147 Cong. Rec. S10990–02, 20 (2001).²² In the absence of pertinent legislative history, we must, as we have done, rely upon language, grammar, and syntax.

²² We also examined the legislative history prior to the 2001 amendment. According to the co-sponsor of the bill introducing the CFAA, the concept of loss was not meant to be limited solely to the cost of actual repairs. Instead, it includes "the cost of computer time necessitated while repairs are being made." 132 Cong. Rec. S14453 (daily ed. Oct. 1, 1986) (statement of co-sponsor Sen. Trible); see also *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 522 n.29 (S.D.N.Y. 2001). In describing the 1994 amendments to the CFAA, another Senate Report touched on the distinction between damage and loss in the context of a hacker who steals information but afterwards restores the altered system to its original condition. In that circumstance, when "the system administrator [must] devote resources to resecuring the system . . . although there is arguably no 'damage,' the victim does suffer 'loss.'" S. Rep. No. 104-357, at 11 (1996); see also *EF Cultural Travel*, 274 F.3d at 584; *P.C. of Yonkers, Inc. v. Celebrations! The Party and Seasonal Superstore, LLC*, Civ. A. No. 04-4554, 2007 WL 708978, at *5 (D.N.J. Mar. 5, 2007).

Teva contends that the defendants' accessing its protected computers instigated the internal investigation into Sandhu. The investigation included searching her company-issued laptop and email account.²³

It does not matter that service continued uninterrupted. As we have determined, direct costs of responding to a violation or assessing the damage done are recoverable even without an interruption of service. *E.g., Brown Jordan Int'l*, 846 F.3d at 1174 (quoting *Nexans Wires*, 166 F. App'x at 563). This includes, for example, hiring a consultant to assess the computer damage, even when service continued uninterrupted. *Nexans Wires*, 319 F. Supp. 2d at 475 (quoting *Explorica*, 274 F.3d at 584); see also *Brown Jordan Int'l*, 846 F.3d at 1174. Teva had no idea what damage had been caused or the extent of Sandhu's transfer of confidential information to Desai and Apotex. Teva's investigation was a response to an offense. See *Yoder*, 774 F.3d at 1073–74; *iParadigms*, 562 F.3d at 646.

On the other hand, Teva cannot recover under the CFAA for lost revenue caused by misappropriation of confidential information. It has not alleged that any lost revenue was caused by a service interruption. Losses in the second category are recoverable only if they are related to an interruption of service. Lost revenue, which falls in the second category, is not recoverable under the CFAA unless it was caused by interruption of service. *Nexans Wires*, 319 F. Supp. 2d at 472–78 (holding \$10 million in lost profits caused by misappropriation of confidential data was not recoverable under the CFAA, which permits recovery of lost revenue only when connected to an "interruption of service"); see also *Huber*, 28 F. Supp. 3d at 330 (citing *Advantage*

²³ Compl. ¶ 64.

Ambulance Grp., Inc. v. Lugo, Civ. A. No. 08-3300, 2009 WL 839085, at *3–4, (E.D. Pa. Mar. 30, 2009) (dismissing claim for future lost revenue due to dissemination of trade secrets accomplished by unauthorized access)) (other citations omitted); *Synthes, Inc. v. Emerge Med., Inc.*, 25 F. Supp. 3d 617, 719 (E.D. Pa. 2014) (“[A] claim for future lost revenue due to the dissemination of trade secrets does not qualify as a ‘loss’ under the CFAA.” (citation omitted)); *ReMedPar, Inc. v. AllParts Medical, LLC*, 683 F. Supp. 2d 605, 614 (M.D. Tenn. 2010) (same).

Defend Trade Secrets Act (DTSA)

The DTSA creates a private right of action for the misappropriation of trade secrets. 18 U.S.C. § 1836(b)(1). The DTSA defines “misappropriation” as the “acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means;” or the “disclosure or use” of a trade secret without the consent of the owner. *Id.* §§ 1839(5)(A)–(B).

The defendants argue that the DTSA does not apply because it was enacted after the alleged misappropriation took place. Teva counters that although the defendants acquired and began using its trade secrets prior the effective date of the DTSA,²⁴ the use continued afterwards.²⁵

Because the misappropriated trade secrets were acquired and used before the enactment of the DTSA does not mean the statute does not apply when use continued after enactment. Misappropriation, as defined in the DTSA, includes unauthorized “use,” not just acquisition, of a trade secret. 18 U.S.C. § 1839(5)(B). Thus, one who

²⁴ The DTSA became effective on May 11, 2016. Pub. L. No. 114–153, § 2, 130 Stat. 376 (2016) (codified as amended at 18 U.S.C. § 1831 *et seq.*).

²⁵ See, e.g., Compl. ¶ 70.

acquired and used a trade secret before enactment of the DTSA and continues to use it after enactment is liable. *Brand Energy*, 2017 WL 1105648, at *4 (citations omitted).

Teva alleges that the defendants continued to use its trade secrets after May 11, 2016, the date of the enactment of DTSA. Teva avers specifically that Apotex continues to use the information in the CRL to make purchasing decisions and set production goals that increase its profits and visibility in the marketplace.²⁶ It alleges that Sandhu continued to connect USB drives to her work laptop as late as July 2016.²⁷ It also claims that on August 8, 2016, Sandhu uploaded a spreadsheet to her personal drive covering the regulatory status of “dozens” of pre- and post-approval Teva products and notes regarding correspondence with the FDA.²⁸ These allegations suffice to state a claim for acquisition, use, and continuing use of trade secrets under the DTSA.

Desai and Apotex also argue that Teva fails to state a claim under the DTSA and the PUTSA because the complaint does not identify what trade secrets were misappropriated. On the contrary, Teva’s allegations are sufficient to put the defendants on notice of what Teva alleges the defendants purloined.

Although the DTSA and the PUTSA use different wording to define a trade secret, they essentially protect the same type of information. Both define a trade secret as information that: (a) the owner has taken reasonable means to keep secret; (b) derives independent economic value, actual or potential, from being kept secret; (c) is not readily ascertainable by proper means; and (d) others who cannot readily access it

²⁶ *Id.* ¶ 61.

²⁷ *Id.* ¶ 76.

²⁸ *Id.* ¶ 70.

would obtain economic value from its disclosure or use. 18 U.S.C. § 1839(3); 12 Pa. Stat. § 5302.

The CRL contained confidential comments from the FDA regarding a drug application that Apotex used to “speed the regulatory approval” of its competing generic product.²⁹ The spreadsheet Sandhu uploaded to her personal drive in August 2016 details “the regulatory status of dozens of pre-approval and post-approval products, and notes on confidential communications with the FDA” regarding its active drug submissions.³⁰

These documents contain information that was not available outside Teva because it was classified as confidential and Teva took measures to restrict access to it. Its value was essential to Teva’s maintaining an advantage over its competitors. Apotex can use it to gain a competitive edge on Teva.

Drawing all reasonable inferences in favor of Teva, we conclude it has identified documents that contain trade secrets. Thus, the misappropriation claims under the DTSA and the PUTSA may proceed.

PUTSA Preemption

The defendants argue that Teva’s common law tort claims are preempted by PUTSA to the extent they are based on allegations of misappropriated trade secrets. The defendants are correct that PUTSA preempts “conflicting” state law tort claims that are “based on the same conduct that is said to constitute a misappropriation of trade secrets.” *Alpha Pro Tech, Inc. v. VWR Int’l LLC*, 984 F. Supp. 2d 425, 447 (E.D. Pa.

²⁹ *Id.* ¶¶ 57–61.

³⁰ *Id.* ¶ 70.

2013) (quoting *Youtie v. Macy's Retail Holding, Inc.*, 653 F. Supp. 2d 612, 620 (E.D. Pa. 2009), and citing 12 Pa. Stat. § 5308). They cite section 5308(a) which reads, “[e]xcept as provided in subsection (b), this chapter displaces conflicting tort, restitutionary and other law of this Commonwealth providing civil remedies for misappropriation of a trade secret.” 12 Pa. Stat. § 5308(a).

It is premature to determine whether the tort claims conflict with PUTSA because Teva may pursue alternative theories of liability at this stage. See *Cenveo Corp. v. Slater*, Civ. A. No. 06-2632, 2007 WL 527720, at *3 (E.D. Pa. Feb. 12, 2007) (“[I]f the Court were to dismiss plaintiff's conversion claim and later make the finding that, although plaintiff had proved that defendants took its pricing structure and business proposals, such information was not a protected trade secret . . . , the Court would be in the difficult position of telling the plaintiff that it had no remedy.”). We refrain from deciding whether PUTSA preempts common law tort claims on a motion to dismiss in the absence of a factual record. *N. Am. Commc'ns, Inc. v. Sessa*, Civ. A. No. 14-227, 2015 WL 5714514, at *8 (W.D. Pa. Sept. 29, 2015) (collecting cases).

If Teva is ultimately unsuccessful on its PUTSA claim, it may still pursue its common law tort claims. A jury could find that Teva has not proven one or more elements for PUTSA liability. If so, there is no PUTSA claim to preempt the tort claims. If the tort claims had been prematurely dismissed, Teva would have no remedy for tort claims and the misappropriation of its trade secrets that it may have proven. If Teva is successful on its PUTSA claim and the jury also finds for Teva on its common law tort claims, Teva will not be allowed to receive double recovery. See, e.g., *Cenveo Corp.*, 2007 WL 527720, at *4. Hence, Teva may proceed with its tort claims.

Tortious Interference

Apotex and Desai argue that even if Teva's tort claims are not preempted by PUTSA, it has not stated a tortious interference claim because it fails to allege that they took purposeful action. According to Teva's complaint, Desai received confidential data and trade secrets from Sandhu, knowing that her sharing the information violated her employment contract with Teva. As a result, Teva argues, Apotex is vicariously liable for Desai's tortious interference.

A plaintiff states a claim for tortious interference if: (1) there is a contract between the plaintiff and a third party; (2) the defendant intended to harm the plaintiff by interfering with the contract; (3) the defendant was not privileged or justified in doing so; and (4) the defendant's conduct caused the plaintiff damages. *Phillips v. Selig*, 959 A.2d 420, 429 (Pa. Super. 2008) (citations omitted). Among the factors considered in determining whether the defendant's conduct was improper are the nature of the conduct, the defendant's motive, and the interests the defendant seeks to advance. *Id.* at 429–30 (quoting Restatement (2d) of Torts § 767 (1979)).

Teva alleges that Sandhu was party to a confidentiality agreement with her employer and Desai induced her to breach it by providing him with Teva's confidential information and trade secrets. Teva avers inferentially that Desai intended to use the materials to Apotex's advantage and Teva's disadvantage. As Desai's employer and beneficiary of the information, Apotex may be held liable for torts committed by its employee. These allegations sufficiently state a claim for tortious interference.

Breach of Fiduciary Duty and Aiding and Abetting Breach of Fiduciary Duty

Apotex and Desai contend that they cannot be held liable for aiding and abetting a breach of fiduciary duty because Teva fails to state a claim for Sandhu's underlying breach of her fiduciary duty.³¹ They are wrong.

To establish a claim for aiding and abetting a breach of fiduciary duty, the plaintiff must show: (1) a third party breached a fiduciary duty owed to the plaintiff; (2) the aider and abettor knew of the breach; and (3) the aider and abettor substantially assisted or encouraged the other in effecting that breach. *Chicago Title Ins. Co. v. Lexington & Concord Search & Abstract, LLC*, 513 F. Supp. 2d 304, 317–18 (E.D. Pa. 2007) (citing *Koken v. Steinberg*, 825 A.2d 723, 732 (Pa. Comm. Ct. 2003); Restatement (2d) of Torts § 876(b)).

Here, Teva alleges that Sandhu had a fiduciary duty to it, she breached her duty, Apotex and Desai knew she was breaching the duty owed to her employer, and they encouraged and substantially assisted her in the breach. These allegations sufficiently state claims for Sandhu's breach of her fiduciary duty to Teva, and for Desai and Apotex's aiding and abetting her breach.

Sandhu, Desai, and Apotex argue that the claims for Sandhu's breach of fiduciary duty and for Desai and Apotex's aiding and abetting that breach are barred by the “gist of the action” doctrine. They contend that these claims are premised on Sandhu's breach of her confidentiality agreement. Hence, according to the defendants, Teva's claim against Sandhu is essentially one for breach of contract, not an action in tort.

³¹ Apotex Mot. to Dismiss at 21–22, ECF 26–27.

Pennsylvania's gist of the action doctrine precludes a plaintiff from bringing what is actually a breach of contract claim as a tort claim. *Bruno v. Erie Ins. Co.*, 106 A.3d 48, 60 (Pa. 2014); *Erie Ins. Exch. v. Abbott Furnace Co.*, 972 A.2d 1232, 1238 (Pa. Super. 2009); see also *Jones v. ABN Amro Mortg. Grp., Inc.*, 606 F.3d 119, 123 (3d Cir. 2010). The doctrine maintains the distinction between causes of action founded on the breach of a contractual duty created by the parties' relationship and those based on the breach of a social duty imposed on all individuals by society.

When the parties' obligations are defined by the terms of a contract and not by duties imposed by social policies, a plaintiff may assert only a contract claim. *Bruno*, 106 A.3d at 68; *Erie Ins. Exch.*, 972 A.2d at 1239 (citing *eToll, Inc. v. Elias/Savion Adver.*, 811 A.2d 10, 14 (Pa. Super. 2002)). To state a tort claim where there is a contract, the wrong complained of must be the gist of the action with the contract being only incidental. *Bruno*, 106 A.3d at 66 (quoting *Bash v. Bell Tel. Co. of Pa.*, 601 A.2d 825, 829 (Pa. Super. 1992)).

In determining whether the gist of the action is based on a contract or a tort, we look to the nature of the duty allegedly breached. *Id.* at 63. If the claim arises directly from a breach of a contractual duty created by the parties, it is a contract action. If the claim arises from the violation of a broader social duty imposed by society and not by the parties to the action, it is a tort action. *Id.* Thus, the substance of the allegations in the complaint is of "paramount importance." *Id.* at 68.

The fact that there is a contract between the parties does not necessarily mean that a party's claim for injury or loss resulting from the other party's conduct in performing the contract is a claim for breach of contract. On one hand, a breach of

contract cause of action is based on the breach of a specific executory promise in the contract. *Id.* at 70. On the other hand, a tort action exists where it is alleged that the defendant breached a duty that exists “independently and regardless of the contract,” one that was not created by the parties. *Id.* at 63.

A claim for breach of fiduciary duty and a claim for breach of contract “can only coexist if the fiduciary duty is based on duties imposed as a matter of social policy and . . . not based on a contractual agreement between the parties.” *Synthes*, 25 F. Supp. 3d at 670 n.8 (citing *Bohler-Uddeholm Am., Inc. v. Ellwood Grp.*, 247 F.3d 79 (3d Cir. 2001); and *Alpart v. Gen. Land Partners, Inc.*, 574 F. Supp. 2d 491, 499 (E.D. Pa. 2008)). The obligations that arise under a fiduciary duty are imposed not by mutual consensus but by social policies “embodied in the law of torts rather than the terms of the contract.” *Synthes*, 25 F. Supp. 3d at 666 (quoting *Bohler-Uddeholm*, 247 F.3d at 105) (internal quotation marks omitted). In other words, the fiduciary duty exists independently of a contract.

Here, Teva contends that Sandhu’s collaborating with Desai and Apotex creates tort liability, separate and apart from her contractual obligations not to disclose trade secrets to a competitor. We agree.

Sandhu’s fiduciary duty was not created by her confidentiality agreement. Instead, it arose from her employment relationship. An employee owes the employer a duty of loyalty “to refrain from competing with the principal and from taking action on behalf of, or otherwise assisting, the principal’s competitors throughout the duration of the agency relationship, as well as a duty not to use property or confidential information of the principal for the agent’s own purpose or those of a third party.” *Synthes*, 25 F.

Supp. 3d at 667 (citing Restatement (3d) of Agency §§ 8.04, 8.05 (2006)). The gist of the fiduciary duty action is the breach of the duty of loyalty, not the breach of the confidentiality agreement, which is collateral. *Bohler-Uddeholm*, 247 F.3d at 105. Accordingly, Teva's claim against Sandhu for breach of her fiduciary duty sounds in tort and is not barred by the gist of the action doctrine.

Teva has sufficiently alleged that Apotex, through its agent Desai, encouraged Sandhu to share trade secrets with them in breach of her known duty. At this stage, that is enough. Therefore, we shall deny Apotex's motion to dismiss the claim for aiding and abetting Sandhu's breach of fiduciary duty.

Sandhu, Desai, and Apotex alternatively argue that both the breach of fiduciary duty and the aiding and abetting claims are barred by the economic loss doctrine. The economic loss doctrine provides that "no cause of action exists for negligence that results solely in economic damages unaccompanied by physical injury or property damage." *Excavation Techs., Inc. v. Columbia Gas Co. of Pa.*, 985 A.2d 840, 841 n.3 (Pa. 2009) (citing *Adams v. Cooper Beach Townhouse Cmties., L.P.*, 816 A.2d 301, 305 (Pa. Super. 2003)).

The claims for breach of fiduciary duty and for aiding and abetting that breach have as an element knowledge and intent on the part of the defendants. See Restatement (2d) of Torts § 876(b). They are intentional torts. They do not sound in negligence. Thus, the economic loss doctrine does not apply. See *Knight v. Springfield Hyundai*, 81 A.3d 940, 951–52 (Pa. Super. 2013) (quoting *Excavation Techs.*, 985 A.2d at 841) (the doctrine applies to bar claims sounding in negligence).

Unfair Competition

Without analysis or explanation, Apotex argues that Teva fails to allege “substantial in[ter]ference” with its business “in a way that had tangible market impact.”³² It contends that Teva’s claim that Apotex used Teva’s trade secrets and confidential information to further its own competitive products is conclusory and lacks factual support. Because Teva alleges that Apotex’s misappropriation of its trade secrets caused harm to its commercial relations, it sufficiently states a claim for unfair competition. See *Synthes (U.S.A.) v. Globus Med., Inc.*, Civ. A. No. 04-1235, 2005 WL 2233441, at *8 (E.D. Pa. Sept. 14, 2005) (citing Restatement (3d) of Unfair Competition § 1 (1995)).

Although no Pennsylvania appellate court has formally recognized the common law tort of unfair competition, several lower state courts have, relying on the Restatement (3d) of Unfair Competition § 1 to define its elements. See, e.g., *Babiarz v. Bell Atl.-Pa., Inc.*, No. 1863, 2001 WL 1808554, at *9 (Pa. Com. Pl. July 10, 2001); *Lakeview Ambulance & Med. Servs., Inc. v. Gold Cross Ambulance & Md. Serv., Inc.*, No. 1994-2166, 1995 WL 842000, at *1–2 (Pa. Com. Pl. Oct. 18, 1995). The Third Circuit has predicted that the Pennsylvania Supreme Court would adopt the Restatement. *Acumed LLC v. Advanced Surgical Servs., Inc.*, 561 F.3d 199, 227 & n.29 (3d Cir. 2009) (“[W]e will assume without deciding that Pennsylvania courts would follow [Restatement (3d) of Unfair Competition § 1].”).

Under the Restatement, a defendant is liable for unfair competition if: (1) he engages in deceptive marketing, infringement of trademark or other protectable

³² Apotex Mot. to Dismiss at 22, ECF 27.

intellectual property, misappropriation of trade secrets, or acts or practices that are actionable under federal or state statutes; and (2) his conduct causes harm to the plaintiff's commercial relations. Restatement (3d) of Unfair Competition § 1;³³ see also *Giordano v. Claudio*, 714 F. Supp. 2d 508, 523 (E.D. Pa. 2010) (quoting *Granite State Ins. Co. v. Aamco Transmissions, Inc.*, 57 F.3d 316, 319 (3d Cir. 1995)).

Where the plaintiff claims the defendant misappropriated trade secrets, tortiously interfered with contract, improperly induced its employees, or unlawfully used its confidential information, the plaintiff states a claim for unfair competition. Restatement (3d) of Unfair Competition § 1; see also *Synthes*, 2005 WL 2233441, at *8 (Pennsylvania Supreme Court recognizes a cause of action for unfair competition where there is evidence of "misappropriation as well as misrepresentation" (quoting *Pottstown Daily News Publ'g Co. v. Pottstown Broad. Co.*, 192 A.2d 657, 662 (Pa. 1963)). Teva has done that. Teva alleges that Apotex misappropriated its trade secrets contained in the CRL and the spreadsheet, and that this misappropriation caused harm to its commercial relations. The alleged harm is that Apotex used Teva's trade secrets to advance the market position of a competing generic product, and to make purchase

³³ Section 1 states in full:

One who causes harm to the commercial relations of another by engaging in a business or trade is not subject to liability to the other for such harm unless:

(a) the harm results from acts or practices of the actor actionable by the other under the rules of this Restatement relating to:

- (1) deceptive marketing . . . ;
- (2) infringement of trademarks . . . ;
- (3) appropriation of intangible trade values including trade secrets and the right of publicity . . . ;

or from other acts or practices of the actor determined to be actionable as an unfair method of competition, taking into account the nature of the conduct and its likely effect on both the person seeking relief and the public; or

(b) the acts or practices of the actor are actionable by the other under federal or state statutes, international agreements, or general principles of common law apart from those considered in this Restatement.

Restatement (3d) of Unfair Competition § 1.

decisions and set production goals that increase profits and visibility in the market.³⁴ These allegations state a claim for unfair competition. See Restatement (3d) of Unfair Competition § 1.

Conversion

Sandhu argues that intangible intellectual property cannot be converted. On the contrary, trade secrets are treated as convertible property under Pennsylvania law. *Gladstone Tech., Partners, LLC v. Dahl*, 222 F. Supp. 3d 432, 441 (E.D. Pa. 2016) (quoting *Giordano*, 714 F. Supp. 2d at 524); *Am. Hearing Aid Assocs., Inc. v. GN Resound N. Am.*, 309 F. Supp. 2d 694, 705 (E.D. Pa. 2004) (citation omitted); see also *SI Handling Sys., Inc. v. Heisley*, 753 F.2d 1244, 1255 (3d Cir. 1985) (citing Restatement of Torts § 757, cmt. b (1939)); *Van Prod. Co. v. General Welding & Fabricating Co.*, 213 A.2d 769, 775 (Pa. 1965).

To state a claim for conversion of trade secrets, a plaintiff must allege that: (1) it owns a trade secret; (2) the trade secret was communicated to the defendant within a confidential relationship; and (3) the defendant used the trade secret to the plaintiff's detriment. *Am. Hearing Aid Assocs.*, 309 F. Supp. 2d at 705 (citation omitted).

Teva states a claim for conversion against Sandhu. It alleges that Sandhu knowingly provided its trade secrets, the CRL and other confidential materials, to Desai and Apotex, who used the trade secrets to compete with Teva, to its detriment. See *Neopart Transit, LLC v. Mgmt. Consulting, Inc.*, Civ. A. No. 16-3103, 2017 WL 714043, at *14 (E.D. Pa. Feb. 23, 2017) (denying motion to dismiss conversion claims based on allegation that former employee provided defendant with information in violation of

³⁴ Compl. ¶¶ 59–61.

confidentiality agreement by downloading email files and other documents to a USB drive and giving them to defendants).

Teva fails to state a claim for conversion against Desai and Apotex. Neither Desai nor Apotex was allegedly in a confidential relationship with Teva. Instead, they were competing with Teva. See Restatement of Torts § 757, cmt. j. Thus, we shall deny the motion to dismiss the conversion claim against Sandhu, but grant the motions as to Desai and Apotex.

Procuring Information By Improper Means

Finally, the defendants contend Teva has failed to state a claim for procuring information by improper means.³⁵ Teva counters that Desai and Apotex secured Teva's trade secrets and confidential information through improper means—the receipt of Sandhu's email and access to her cloud drive. Sandhu argues that she properly acquired the protected materials through the course of her employment.³⁶ Teva counters that Sandhu's conduct was improper because she accessed and copied its trade secrets, in violation of her employment agreement and Teva's policies, and disclosed them to a competitor.

When the defendant, "for the purpose of advancing a rival business interest, procures by improper means information about another's business[, he] is liable to the other for the harm caused by his possession, disclosure or use of the information."

Pestco, Inc. v. Associated Prod., Inc., 880 A.2d 700, 708–09 (Pa. Super. 2005) (quoting

³⁵ Apotex Mot. to Dismiss at 24, ECF 29.

³⁶ Sandhu Mot. to Dismiss (Doc. No. 50) at 13, ECF 17.

Restatement (2d) of Torts § 759). An allegation that the defendant improperly procured confidential business information, causing harm to the plaintiff, suffices to state a claim.

Teva alleges that Apotex, through Desai, improperly procured the CRL and other confidential information from Sandhu, and used that information to gain a competitive advantage. These allegations state a cause of action against Desai and Apotex for procuring information by improper means.

The claim against Sandhu, however, must be dismissed. Teva alleges that she procured the information while employed there. It does not allege that she got it by improper means. Indeed, as we have seen, she was authorized to procure the information.

Count Seeking Permanent Injunction

An injunction is a remedy rather than a cause of action. A separate claim for injunctive relief is unnecessary. See, e.g., *Birdman v. Office of the Governor*, 677 F.3d 167, 172 (3d Cir. 2012). Thus, Count XI shall be dismissed.